UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/626,637	07/27/2000	Deepak Gupta	JP920000150US1	9799

39903 7590 10/10/2006

ANTHONY ENGLAND
PO Box 5307
AUSTIN, TX 78763-5307

EXAMINER	
SHIN, KYUNG H	

ART UNIT	PAPER NUMBER
2143	

DATE MAILED: 10/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/626,637
Filing Date: 7/27/2000
Appellant(s): GUPTA, DEEPAK ET AL

Jack P. Friedman
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 7/17/2006 appealing from the Office action mailed 8/11/2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,233,565	Lewis et al.	5-2001
6,094,485	Weinstein et al.	7-2000
6,230,266	Perlman et al.	5-2001
6,324,525	Kramer et al.	11-2001

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

DETAILED ACTION

1. Claims **1 - 6, 11 - 19** are pending. Claims **1 - 5** are amended. Claims **7 - 10** are cancelled. Claims **11 - 19** are new. Independent claims are **1, 6, 13**.

Claim Rejection - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. **Claims 1, 4 - 6, 11, 13, 17 - 19** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Lewis et al.** (US Patent No. 6,233,565) in view of **Weinstein et al.** (US Patent No. 6,094,485).

Regarding Claim 1 (Currently Amended), Lewis discloses a method for enabling the use by a browser of valid authentication certificates in relation to a transaction between the browser and a server when a private key and public key of a certifying authority of the server has expired, comprising:

b) verifying by the browser the original authentication certificate using the expired public key of the certifying authority, (see Lewis col. 14, lines 36-42; col. 30, lines 41-43: verify certificate by (i.e. client) browser using expired public key for verification and utilize expired private key for digital signature generation) and

c) verifying by the browser the SCAC certificate using a new public key of the certifying authority. (see Lewis col. 30, lines 43-50: verify certificate by (i.e. client) browser using new public key for verification and new private key for digital signature generation)

Lewis discloses wherein receiving an original authentication certificate and a server certifying authority chain (SCAC) certificate by the browser from the server during a SSL handshake between the browser and the server, said SCAC certificate having been previously obtained by the server from the certifying

authority (see Lewis col. 30, lines 39-41; col. 14, lines 36-42; col. 15, lines 42-46: receive original certificate, new certificate utilizing SSL techniques)

Lewis does not specifically disclose certificates received together. However, Weinstein discloses:

a) receiving an original authentication certificate together with a server certifying authority chain (SCAC) certificate. (see Weinstein col. 3, lines 56-64: multiple (i.e. new, intermediate (i.e. old)) certificates within a transmission (i.e. together))

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Lewis to enable multiple security client/server certificates transmitted within a network session as taught by Weinstein. One of ordinary skill in the art would be motivated to employ Weinstein in order to optimize encryption within a secure network communications session. (see Weinstein col. 2, lines 10-15: " *... provides a process and apparatus that is used by an exportable version of an SSL client ... negotiate an encrypted communication session using strong encryption with an SSL server ...* ")

Regarding Claim 5 (Currently Amended), Lewis discloses the method of claim 1, wherein the method further comprises presenting the CCAC certificate to the server during the handshake. (see Lewis col. 14, lines 36-42; col. 15, lines 42-46; col. 31, lines 5-21: certificate to contain client public/private key pair generated and client certificate setup utilizing handshake (i.e. SSL) techniques)

Regarding Claim 6 (Original), Lewis discloses in an arrangement of networked server and browser systems conducting secure transactions and including a certifying authority for authenticating such transactions, characterized in that it includes a means for authenticating transactions when the public and private key of the said certifying authority have expired but the authentication certificates of any of server or browser systems is still valid, comprising;

a) a means for the server to obtain a certifying authority chain certificate using the new private key of the certifying authority, (see Lewis col. 30, lines 39-41: server receives a new certificate designating a new private key)

c) a means for verifying the original authentication certificate using the expired public key of the certifying authority, and verifying the certifying authority chain certificate using the new certifying authority public key by the browser. (see Lewis col. 30, lines 43-50: initial certificate signed with expired private key (i.e. verified with expired public key), new certificate signed with new private key (i.e. verified with new public key))

Lewis discloses the usage of original and new certificates. (see Lewis col. 14, lines 36-42; col. 30, lines 41-43: certificates utilized for authenication) Lewis does not specifically disclose certificates received together. However, Weinstein discloses:

b) a means for presenting the said certifying authority chain certificate together with the original authentication certificate, to the browser; (see Weinstein col. 3, lines 56-64: multiple (i.e. new, intermediate (i.e. old)) certificates within a transmission)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Lewis to enable multiple security client/server certificates transmitted within a network session as taught by Weinstein. One of ordinary skill in the art would be motivated to employ Weinstein in order to optimize encryption within a secure network communications session. (see Weinstein col. 2, lines 10-15)

Regarding Claims 11 (New), **18** (New), Lewis discloses the method and system of claims 1, 13 further comprising accepting the transaction by the browser after said verifying the original authentication certificate and after said verifying the SCAC certificate. (see Lewis col. 27, lines 10-24: verification of a certificate (i.e. server or client) utilizing digital signature techniques with public/private keys)

Regarding Claims 12 (New), **19** (New), Lewis disclose the method and system of claims 1, 13, wherein obtaining the SCAC certificate comprises using the new private key of the certifying authority. (see Lewis col. 30, lines 41-43: certificate (i.e. server/client) utilizing private key for digital signature generation and public key for verification)

Regarding Claim 13 (New), Lewis discloses a system for enabling use by a browser of valid authentication certificates in relation to a transaction between the browser and a

server when a private key and public key of a certifying authority of the server has expired, comprising:

b) means for verifying by the browser the original authentication certificate using the expired public key of the certifying authority; (see Lewis col. 30, lines 43-50: initial certificate signed with expired private key (i.e. verified with expired public key), new certificate signed with new private key (i.e. verified with new public key)) and

c) means for verifying by the browser the SCAC certificate using a new public key of the certifying authority. (see Lewis col. 30, lines 39-41: server receives a new certificate designating a new private key)

Lewis discloses wherein means for receiving an original authentication certificate and a server certifying authority chain (SCAC) certificate by the browser from the server during a SSL handshake between the browser and the server, said SCAC certificate having been previously obtained by the server from the certifying authority; (see Lewis col. 30, lines 39-41; col. 14, lines 36-42; col. 15, lines 42-46: receive original certificate, new certificate utilizing SSL techniques) Lewis does not specifically disclose certificates received together. However, Weinstein discloses:

a) receiving an original authentication certificate together with a server certifying authority chain (SCAC) certificate. (see Weinstein col. 3, lines 56-64: multiple (i.e. new, intermediate (i.e. old)) certificates within transmission)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Lewis to enable multiple security client/server certificates transmitted within a network session as taught by Weinstein. One of ordinary skill in the art would be motivated to employ Weinstein in order to optimize encryption within a secure network communications session. (see Weinstein col. 2, lines 10-15)

Regarding Claim 17 (New), Lewis discloses the system of claim 13, wherein the system further comprises means for presenting the CCAC certificate to the server during the handshake. (see Lewis col. 14, lines 36-42; col. 15, lines 42-46; col. 31, lines 5-21: certificate to contain client public/private key pair generated and client certificate setup utilizing handshake (i.e. SSL) techniques)

4. **Claims 2, 3, 14, 15** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Lewis-Weinstein** and further in view of **Perlman et al.** (US Patent No. 6,230,266).

Regarding Claim 2 (Currently Amended), Lewis discloses a Certificate Authority (CA) for the distribution of certificates used in the verification of client and server systems. Lewis does not disclose a Certificate Authority (CA) that invalidates or withdraws its public/private key. However, Perlman discloses Certificate Authority (CA) that invalidates or withdraws its public/private key pair through the process of revocation.

Further, Perlman discloses the method of claim 1, wherein the SCAC certificate is obtained by the server whenever the certifying authority invalidates its public key, wherein the certificate is obtained by:

a) contacting the certifying authority using the server's private key for authentication to make a request for the SCAC certificate; (see Perlman col. 6, line 63 - col. 7, line 6: contact CA concerning certificate revocation)

b) verifying the request by the certifying authority using the server's public key; (see Perlman col. 7, lines 15-18: verify key revocation) and

c) generating the SCAC certificate by the certifying authority using it's new private key of the certifying authority and forwarding the SCAC certificate to the server. (see Perlman col. 7, lines 12-24: update certificate information, attach key to new certificate)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inventions of Lewis to include a Certificate Authority (CA) that invalidates its key pair through the process of revocation as taught by Perlman. One of ordinary skill in the art would have been motivated to employ Perlman in order to ensure the authenticity of certificates when a CA invalidates a public/private key pair. (see Perlman col. 2, lines 20-26: " *... network security, every principal must have a certificate ... desirable to later disable a certificate after it has been issued but prior to its expiration. For example, a principal's private key may be stolen, compromised or lost, etc. ... revoke the certificate, thereby disabling authentication via that certificate ...* ")

Regarding Claim 3 (Currently Amended), Lewis discloses a Certificate Authority (CA) for the distribution of certificates used in the verification of client and server systems and an entity (i.e. server) name for a certificate. (see Lewis col. 26, line 56: entity (i.e. server) name within certificate) Lewis does not disclose usage of the server public key, CA name and public key in the authentication process. However, Perlman discloses the method of claim 2 wherein generating the SCAC certificate includes authenticating the server public key, old certifying authority public key and certifying authority name. (see Perlman col. 7, lines 10-12: public keys, CA name)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inventions of Lewis to include the invention of Perlman enable usage. One of ordinary skill in the art would have been motivated to employ the invention of Perlman to Lewis in order to use efficiently the server name and public key, CA name and public key authentication. (see Perlman col. 1, line 65 - col. 2, line 9: " ... *reliably know which public key belongs to which principal ... CA generates identity certificates ... specifying ... name of the principal whose public key is being certified, the certificate serial number, name of the CA issuing the certificate, the subject's public key, and also, typically, a certificate expiration date ... relationship between the public key and the principal to which it belongs precludes an intruder from compromising the system by posing as a valid principal ...* " ; col. 7, lines 10-12: " ... *new CA 204b is configured to issue certificates in the same name as the CA 204a ...* ") The compromise of a CA and its identifying information requires another CA and its

identifying information to assume the certificate verification process.

Regarding Claim 14 (New), Lewis does not disclose a Certificate Authority (CA) invalidation of it public/private key. However, Perlman discloses the system of claim 13, wherein the SCAC certificate is obtained by the server whenever the certifying authority invalidates its public key, wherein the certificate is obtained by:

a) means for contacting the certifying authority using the server's private key for authentication to make a request for the SCAC certificate; (see Perlman col. 6, line 63 - col. 7, line 6: contact CA concerning certificate revocation)

b) means for verifying the request by the certifying authority using the server's public key; (see Perlman col. 7, lines 15-18: verify key revocation) and

c) means for generating the SCAC certificate by the certifying authority using a new private key of the certifying authority and forwarding the SCAC certificate to the server. (see Perlman col. 7, lines 12-24: update certificate information, attach key to new certificate)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inventions of Lewis to include a Certificate Authority (CA) that invalidates its key pair as taught by Perlman. One of ordinary skill in the art would have been motivated to employ Perlman in order to ensure the authenticity of certificates when a CA invalidates a public/private key pair to a compromise in security. (see Perlman col. 2, lines 20-26)

Regarding Claim 15 (New), Lewis discloses a Certificate Authority (CA) for the distribution of certificates used in the verification of client and server systems. Lewis discloses an entity (i.e. server) name for a certificate. (see Lewis col. 26, line 56: entity (i.e. server) name within certificate) Lewis does not specifically disclose usage of the public key, CA name and public key in the authentication process. However, Perlman discloses the system of claim 13, wherein said means for generating the SCAC certificate includes means for authenticating the server name, the server public key, old certifying authority public key, and certifying authority name. (see Perlman col. 7, lines 10-12: public keys, CA name)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inventions of Lewis to employ the certificates includes the authentication of the server public key, old CA public key and CA name as taught by Perlman. One of ordinary skill in the art would have been motivated to employ Perlman in order to efficiently and securely re-establish authentication system by using the server name and public key, CA name and public key authentication. (see Perlman col. 3, lines 54-63)

5. **Claim 4** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Lewis-Weinstein** and further in view of **Kramer et al.** (US Patent No. 6,324,525).

Regarding Claim 4 (Currently Amended), Lewis discloses the usage of certificates for entity authentication. (see Lewis col. 31, lines 35-38: client/server certificate usage for

authentication) Lewis does not specifically disclose the usage of a Certificate Authority (CA) issuing client and server type certificates. However, Kramer discloses the method of claim 1 further comprising issuing by the certifying authority a client (CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged. (see Kramer col. 105, lines 61-62; col. 105, line 66 - col. 106, line 1; col. 90, lines 27-31: Certificate Authority (CA) for certificate issuance; col. 17, lines 43-47; col. 17, lines 27-30: client and server type certificates)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Lewis to enable the usage of client and server certificates utilizing a trusted third party designated a certificate authority for certificate issuance as taught by Kramer. One of ordinary skill in the art would be motivated to employ Kramer in order to enable secure communications over the publicly access network such as the Internet communications network. (see Kramer col. 4, lines 19-21: " *... critical that any solution utilizing the Internet for a communication backbone employ some form of cryptography ...* ")

6. **Claim 16** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Lewis-Weinstein-Perlman** and further in view of **Kramer et al.** (US Patent No. 6,324,525).

Regarding Claim 16 (New), Lewis discloses the usage of certificates for entity authentication. (see Lewis col. col. 30, lines 59-62:) Lewis does not specifically

disclose the usage of a Certificate Authority issuing client and server type certificate. However, Kramer discloses the system of claim 15, further comprising means for issuing by the certifying authority a client (CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged. (see Kramer col. 105, lines 61-62; col. 105, line 66 - col. 106, line 1; col. 90, lines 27-31: Certificate Authority (CA) for certificate issuance; col. 17, lines 43-47; col. 17, lines 27-30: client and server certificates)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Lewis to enable the usage of client certificates and server certificates utilizing a trusted third party designated a certificate authority for certificate issuance as taught by Kramer. One of ordinary skill in the art would be motivated to employ Kramer in order to enable secure communications over the publicly access network such as the Internet communications network. (see Kramer col. 4, lines 19-21)

(10) Response to Argument

A. As to claims **1, 5 - 6, 11 - 13, 17 - 19**, applicant argues in substance that:

A.1. The referenced prior art does not disclose " *... receiving an original authentication certificate together with a server certifying authority chain (SCAC) certificate by the browser from the server during a SSL handshake between the browser and the server, said SCAC certificate having been previously obtained by*

the server from the certificate authority ... " (see Appeal Brief Page 5, Lines 12-15)

A.2. The referenced prior art does not disclose *" ... the old certificate and the new certificate are not received by the browser from the server as required by claims 1, 6, 13, but are instead received by the server from the Certificate Authority ... " (see Appeal Brief Page 7, Lines 4-6)*

A.3. The referenced prior art does not disclose *" ... verifying by the browser the original authentication certificate using the expired public key of the certificate authority ... " (see Appeal Brief Page 7, Lines 18-19)*

A.4. The referenced prior art does not disclose the limitations of claims 11, 12, 18, 19 due to the patentability of claims 1 and 13.

B. As to claims **2, 3, 14, 15**, applicant argues in substance that:

B.1. The referenced prior art does not disclose *" ... wherein the SCAC certificate is obtained by the server whenever the certifying authority invalidates its public key ... " (see Appeal Brief Page 11, Line 11-13)* ; *" ... repeatedly discusses certificate revocation. However, Perlman does not teach or suggest public key invalidation, and the Examiner has not produced a citation that allegedly discloses public key invalidation ... " (see Appeal Brief Page 11, Lines 18-19)*

B.2. The referenced prior art does not disclose *" ... to make a request for the SCAC certificate ... " (see Appeal Brief Page 13, Lines 3-4)*

B.3. The referenced prior art does not disclose *" ... generating the SCAC certificate includes authenticating the server name, the server public key, old certifying*

authority public key, and certifying authority name ... " (see Appeal Brief Page 15, Lines 9-11)

C. As to claims **4**, applicant argues in substance that:

C.1. The referenced prior art does not disclose *" ... issuing by the certificate authority a client (CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged ... " (see Appeal Brief Page 17, Lines 8-10) ; " ... does not specifically disclose the usage of a Certificate Authority (CA) issuing client and server type certificates ... " (see Appeal Brief Page 17, Lines 11-12)*

D. As to claims **16**, applicant argues in substance that:

D.1. The referenced prior art does not disclose *" ... issuing by the certificate authority a client (CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged ... " (see Appeal Brief Page 20, Lines 8-11)*

Examiner's Response to Argument dated 11/11/2005

The examiner's rejection is proper given that the cited passages of Lewis, Weinstein, Perlman, Kramer disclose the applicant's invention.

As to Point A.1.

Applicant's invention calls for the implementation of a new certificate when a cryptographic key attached to the current certificate has expired or is invalided. The expiration of cryptographic keys is an ongoing situation in an online operational system. The "original" certificate must be the "current" certificate attach to a public/private key pair. The true original certificate and its public/private key will be invalid a long time ago.

The Lewis prior art discloses receiving an original authentication certificate and a server certifying authority chain (SCAC) certificate by the browser from the server utilizing SSL data transmission techniques. Lewis discloses server certificate being obtained from the certificate authority by the server (see Lewis col. 30, lines 39-41; col. 14, lines 36-42; col. 15, lines 42-46: receive original certificate, new certificate utilizing SSL techniques)

Lewis in view of Weinstein discloses the receipt of multiple certificates within one transmission. Therefore, ~~it~~ the referenced prior art discloses receiving an original authentication certificate together with a server certifying authority chain certificate. (see Weinstein col. 3, lines 56-64: multiple (i.e. new, intermediate (i.e. old)) certificates within a transmission (i.e. together))

As to Point A.2.

A server is a system that provides a service to a client system. In addition, when a

server system receives a service from another system, it becomes a client to that particular system. The server and client roles are interchangeable based on which system is requesting the service and which system is receiving the service. A server system can be a server in one situation and that same server can be a client in another situation. Lewis discloses the capability to receive a certificate by a client or a server. (see Lewis col. 30, lines 39-41; col. 14, lines 36-42; col. 15, lines 42-46: receive original certificate, new certificate) A.1 discloses the receipt of the old certificate and the new certificate in one data transmission.

As to Point A.3.

The Lewis prior art discloses the capability to verify an original authentication certificate using the expired public key of the certifying authority. In addition, Lewis prior art discloses verifying the certifying authority chain certificate using the new certifying authority public key by the browser. (see Lewis col. 30, lines 43-50: initial certificate signed with expired private key (i.e. verified with expired public key), new certificate signed with new private key (i.e. verified with new public key))

As to Point A.4.

Applicant contends that the patentability of claims 11, 18, 12, 19 is based on the patentability of independent claims 1, 13.

Independent claims 1 and 13 are rejected based on the referenced prior art. In addition, claims 11, 12, 18, 19 are rejected due to rejection of the base independent

claims 1 and 13.

As to Point B.1.

The revocation of a public/private key is analogous to the invalidation of a certificate and its public/private key pair. The reason for the revocation can be an expired key pair, compromise of a key pair, or any other reason the certificate authority is required to invalidate or revoke the public/private key pair and its attached certificate.

As to Point B.2.

Lewis discloses a Certificate Authority (CA) for the distribution of certificates used in the verification of client and server systems and an entity (i.e. server) name for a certificate. (see Lewis col. 26, line 56: entity (i.e. server) name within certificate)

As to Point B.3.

Lewis prior art discloses a Certificate Authority (CA) for the distribution of certificates used in the verification of client and server systems and discloses one of the required entities, the (i.e. server) name of the certificate. (see Lewis col. 26, line 56: entity (i.e. server) name within certificate) Lewis in view of Perlman discloses generating the SCAC certificate includes the following actions including an authenticating the following items, the server public key, old certifying authority public key and the certifying authority name. (see Perlman col. 7, lines 10-12: public keys, CA name) Lewis in view of Perlman discloses all four of the required items for certificate

authentication.

As to Point C.1.

Lewis in view of Kramer discloses, further comprising means for issuing by the Certifying Authority a client certificate, said client certificate being functionally the same as the server certificate subject to the roles of the browser and the server being interchanged. (see Kramer col. 105, lines 61-62., col. 105, line 66 - col. 106, line 1; col. 90, lines 27-31: Certificate Authority (CA) for certificate issuance; col. 17, lines 43-47; col. 17, lines 27-30: client and server certificates)

As to Point D.1.

Response to Point C.1 is the same response as the response to D.1.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

KHS
Kyung H Shin
Patent Examiner
Art Unit 2143

KHS
9/26/06

Conferees:

***

BUNJOB JAROENCHONWANIT
SUPERVISORY PATENT EXAMINER

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100